OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

A Common Cyber Threat Framework:
A Foundation for Communication

LEADING INTELLIGENCE INTEGRATION

With So Many Cyber Threat Models or Frameworks

Why build another?

Intent
Reconnaissance
Resource development
Staging

Target ID
Exploitation
Delivery

Maintain/expand Target access
Detection voidance
Establish/modify Network infrastructure
C2

Deny Access
Extract Data
Manipulate

Administer | Prepare | Engage | Propagate | Effect

Intent | Reconnaissance | Development | Staging | Delivery | Configure | Maneuver | Exploitation | C2 | Effect

Foot printing | Scanning | Enumeration | Gain access (exploitation) | Privilege escalation | Situational awareness | Covering tracks | Creating Backdoors

Malware | Hacking | Social | Environmental threat | Physical threat | Misuse | Error

Actor | Tactics, Techniques, & Procedures | Infrastructure | Victim

Reconnaissance | Weaponization | Delivery | Exploitation | Installation | C2 | Actions on Objective

Lockheed Martin Kill Chain ®

Intent | Development | Reconnaissance | Staging | Engagement | Maneuver | Configure | C2 | Effect

STIX™

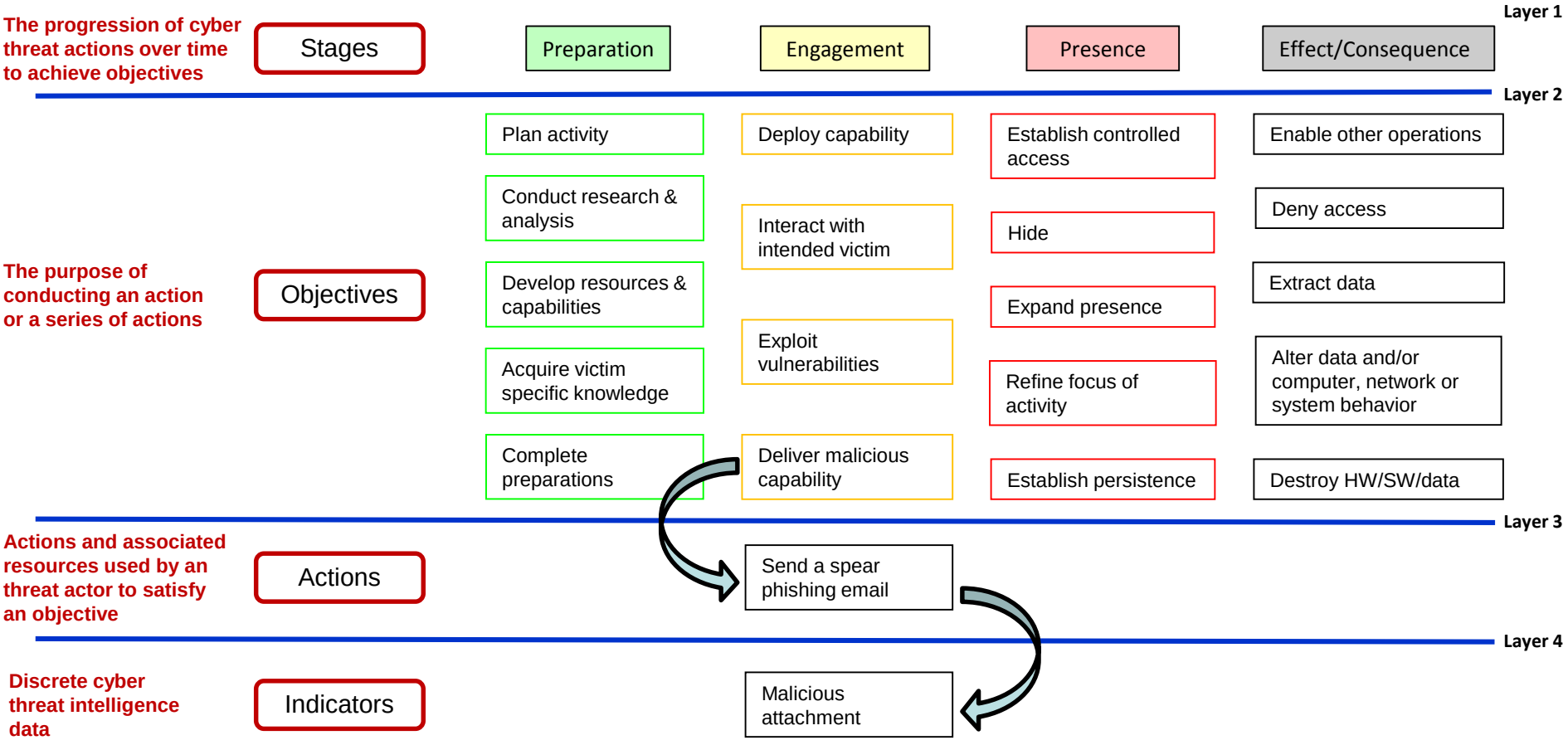
… Because comparison of threat data across models and users is problematic

Following a common approach helps to:

- ***Establish a common ontology*** and ***enhance information-sharing*** since it is easier to map unique models to a common standard than to each other
- ***Characterize and categorize threat activity*** in a straightforward way that can support missions ranging from strategic decision-making to analysis and cybersecurity measures and users from generalists to technical expert
- ***Achieve common situational awareness*** across organizations

Common Cyber Threat Framework

Hierarchical, Structured, Transparent and Repeatable



This Common Approach Facilitates Grouping and Comparison of Cyber Threat Activities Seen from Different Perspectives